## REMARKS/ARGUMENTS

***Applicant' undersigned attorney requests an interview with the Examiner once the Examiner has had an opportunity to review the remarks submitted herein.***

Claims 1, 18-21, and 23-29 are amended herein. Claims 1, 3, 5-21, and 23-29 are currently pending.

Claims 1, 3, 5-21, and 23-29 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2005/0097203 (Unbehagen et al.) and U.S. Patent No. 7,120,792 (Jacobson et al.)

Claim 1 is directed to a method of establishing a BGP mesh in a network. The method includes, inter alia, receiving BGP peering information flooded from a network device, automatically discovering at least one neighbor utilizing the received BGP peering information, and automatically establishing a BGP peering session with the neighbor to establish a BGP mesh. The flooded BGP peering information includes static configuration parameters used to establish the BGP peering session. The claims have been amended to clarify that the BGP peering information is flooded from a BGP speaker.

Unbehagen et al. disclose an auto discovery for virtual networks which facilitates discovery of VPN-related information. VPN information is discovered in an already established BGP session. Rather than receiving BGP peering information, discovering a neighbor, and establishing a BGP peering session, as set forth in the claims, Unbehagen et al. utilize an existing BGP session to communicate VPN information between network devices.

Furthermore, Unbehagen et al. do not show or suggest receiving BGP peering information flooded from a network device. In rejecting the claims, the Examiner refers to paragraphs [0019] and [0020] of Unbehagen et al. This section of the patent application describes how BGP is used to communicate information to support VPN.

There is already a connection between two devices and BGP is used to transmit VPN information.

Also, Unbehagen et al. do not disclose receiving BGP peering information comprising static configuration parameters used to establish a BGP peering session.

Moreover, Unbehagen et al. do not show or suggest automatically discovering at least one neighbor utilizing received BGP peering information or automatically establishing a BGP peering session with the neighbor. In rejecting the claims, the Examiner refers to paragraphs [005] and [0020] of Unbehagen et al. Paragraph [005] notes that BGP may be used to allow provider edge devices to negotiate capabilities. Paragraph [0020] describes how BGP is used to communicate information to support VPN. As noted above, there is no discussion of discovering neighbors or creating BGP sessions. The patent application simply describes how BGP is used to communicate VPN information.

Conventional systems such as Unbehagen et al. establish BGP neighbors (or peers) by manual configuration between routers. Manual configuration of routers for establishment of a full mesh constitutes a significant operational problem in terms of configuration management. Applicant's invention, as set forth in the claims, uses flooding of BGP peer information which includes static configuration parameters. This peer information is then used to automatically discover at least one neighbor. This allows for automatic establishment of a BGP peering session.

As noted by the Examiner Unbehagen et al. do not teach flooded BGP peering information.

Jacobson et al. disclose a system for secure communication of routing messages. The system distributes encryption or authentication capabilities among route processors so that the route processors can back each other up. When the system is initialized, a series of BGP conversations are initiated using conventional BGP protocols. Encryption or authentication information such as cryptographic parameters is flooded to neighbor devices. Thus, a BGP session is already established and the flooding is used to transmit a

BGP message to devices in which a BGP session has already been established. Rather than flooding BGP peering information, as set forth in the claims, Jacobson et al. simply flood BGP messages after a session has been established. Furthermore, messages are only flooded to peers, whereas messages to non-peers are provided via a conventional TCP/TP connection. In contrast to applicant's claimed invention, which floods static configuration parameters used to establish a peering session, Jacobson et al. only use flooding for transmitting messages (after a session has been established) with peer nodes. As noted by the Examiner, Jacobson et al. reduces the resources required to communicate routing information. The BGP routing information is communicated after the BGP session has been established. The claimed invention requires the flooding of static configuration parameters used to establish a BGP peering session, not the transfer of routing information in an established BGP session.

Applicant's claimed flooding of static parameters by BGP speakers allows for automatic discovery of potential peers so that BGP peering sessions can be established. The Examiner has failed to point to any teaching of flooding static configuration parameters used to establish a BGP peering session, from a BGP speaker.

In the Response to the Arguments, the Examiner simply refers to col. 4, lines 53-67 of Jacobson et al and states that "Jacob teaches BGP processor capable of processing messages and exchange sync information (which can be static parameters as known in the art) *during BGP sessions*." (emphasis added). Applicant's claims specify that the flooded information is used to establish a BGP peering session, which is not shown or suggested by Jacobson et al.

Accordingly, claim 1 is submitted as patentable over the cited references.

Claims 3 and 5-17, depending either directly or indirectly from claim 1, are submitted as patentable for at least the same reasons as claim 1.

Claims 18-21 and 23-29, as amended, are submitted as patentable for at least the same reasons as claim 1.

Claim 5 is further submitted as patentable over the cited references which do not show or suggest BGP peering information comprising a BGP identifier. In rejecting the claims, the Examiner refers to paragraph [0026] of Unbehagen et al. This paragraph describes a VPN identifier rather than a BGP identifier associated with BGP peering information.

With regard to claim 6, Unbehagen et al. do not flood BGP peer information. Thus, there is no teaching of transmitting or receiving BGP peering information comprising a flooding protocol.

Claims 7 and 8 are further submitted as patentable of Jacobson et al., which do not teach an OSPF or ISIS flooding protocol or a flooding scope.

With regard to the limitations of claims 10-16, the Examiner has failed to point to any teaching of the specific BGP peering information as set forth in the claims. As discussed above, Unbehagen et al. do not discuss BGP peering information used to establish a BGP peering session. Thus, none of the specific BGP peering limitations set forth in the claims are taught by Unbehagen et al.

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,

Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-399-5609